Amendments to the Claims

Claims 1 - 2 (canceled)

Claim 3 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is an executable method.

Claim 4 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a column of a database table.

Claim 5 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a row of a database table.

Claim 6 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a file and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are file access operations that can be performed on the file.

Claim 7 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a function call to a function of an executable program.

Claim 8 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is an Enterprise JavaBean ("EJB") and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are methods that can be performed on the EJB.

Claim 9 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a servlet and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are methods that can be performed by [[of]] the servlet.

Claim 10 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a Uniform Resource Identifier ("URI") and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are methods which reference the URI.

Claim 11 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is a JavaServer Page ("JSP") and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are methods referenced from the JSP.

Claim 12 (currently amended): The method according to Claim [[1]] 19, wherein at least one of the resources is any resource that is expressible to the security system and each of the at least one ~~the permitted~~ actions [[on]] identified for the at least one resource are selected from a set of actions that are permitted on that resource.

Claims 13 - 18 (canceled)

Claim 19 (new): A computer-implemented method for enforcing role-permission security administration using security objects stored in a security repository, comprising steps of:

storing, in a security repository, a plurality of security objects, wherein each of the security objects corresponds to a single role;

specifying, in each of the security objects, all permissions granted to the corresponding role, wherein each of the specified permissions identifies at least one resource and, for each resource, at least one action that can be performed on the resource by subjects granted the corresponding role, wherein selected ones of the resources are identified in the specified permissions of more than one of the security objects and wherein the specified permissions for at least one of the security objects identifies a plurality of resources and for each of the plurality of resources, at least one of the actions; and

using the stored security objects to determine whether run-time requests for performing actions on the resources can be granted.

Claim 20 (new): The method according to Claim 19, where the using step further comprises, for each of the run-time requests, the steps of:

determining, for the run-time request, a requester from which the request was received, and a particular action being requested on a particular resource;

determining one or more roles granted to the requester; and

until determining that the request can be granted or exhausting the determined roles, iteratively accessing the security object corresponding to each one of the determined roles and if the accessed security object identifies the requested action on the requested resource, then determining that the request can be granted.

Claim 21 (new): The method according to Claim 20, wherein the step of determining one or more roles further comprises the steps of:

using an identification of the requester as a user identification to consult a mapping that specifies, for each of a plurality of subjects, one or more roles associated therewith, wherein each of the subjects is specified as at least one of (1) an identification of one or more users and (2) an identification of one or more user groups, thereby determining each role associated with the identification of the requester;

determining one or more user groups of which the requester is a member; and

using each of the determined user groups as a user group identification to consult the mapping, thereby determining each role associated with the determined user groups.

Claim 22 (new): The method according to Claim 19, where the using step further comprises, for each of the run-time requests, the steps of:

determining, for the run-time request, a requester from which the request was received, and a particular action being requested on a particular resource; and

determining that the run-time request can be granted only if the requester has been granted at least one of the roles which is required, according to the stored security objects, to perform the requested action on the requested resource.

Claim 23 (new): A system for enforcing role-permission security administration using security objects stored in a security repository, comprising:

a security repository for storing a plurality of security objects, wherein each of the

security objects corresponds to a single role;

means for specifying, in each of the security objects, all permissions granted to the corresponding role, wherein each of the specified permissions identifies at least one resource and, for each resource, at least one action that can be performed on the resource by subjects granted the corresponding role, wherein selected ones of the resources are identified in the specified permissions of more than one of the security objects and wherein the specified permissions for at least one of the security objects identifies a plurality of resources and for each of the plurality of resources, at least one of the actions; and

means for using the stored security objects to determine whether run-time requests for performing actions on the resources can be granted.

Claim 24 (new): The system according to Claim 23, where the means for using further comprises means for performing, for each of the run-time requests, steps of:

determining, for the run-time request, a requester from which the request was received, and a particular action being requested on a particular resource;

determining one or more roles granted to the requester; and

until determining that the request can be granted or exhausting the determined roles, iteratively accessing the security object corresponding to each one of the determined roles and if the accessed security object identifies the requested action on the requested resource, then determining that the request can be granted.

Claim 25 (new): A computer program product for enforcing role-permission security

administration using security objects stored in a security repository, the computer program product comprising computer-readable code embodied on one or more computer-usable media, the computer-readable code comprising instructions that when executed on a computer cause the computer to:

store, in a security repository, a plurality of security objects, wherein each of the security objects corresponds to a single role;

specify, in each of the security objects, all permissions granted to the corresponding role, wherein each of the specified permissions identifies at least one resource and, for each resource, at least one action that can be performed on the resource by subjects granted the corresponding role, wherein selected ones of the resources are identified in the specified permissions of more than one of the security objects and wherein the specified permissions for at least one of the security objects identifies a plurality of resources and for each of the plurality of resources, at least one of the actions; and

use the stored security objects to determine whether run-time requests for performing actions on the resources can be granted.

Claim 26 (new): The computer program product according to Claim 25, where the instructions that cause the computer to use the stored security objects further comprise instructions that cause the computer, for each of the run-time requests, to:

determine, for the run-time request, a requester from which the request was received, and a particular action being requested on a particular resource; and

determine that the run-time request can be granted only if the requester has been granted

at least one of the roles which is required, according to the stored security objects, to perform the requested action on the requested resource.